12. Die Legendre-Gleichung und der Drei-Quadrate-Satz von Gauß

Die Legendre-Gleichung

Unter der Legendre-Gleichung versteht man die Diophantische Gleichung

$$ax^2 + by^2 + cz^2 = 0 \tag{1}$$

Dabei seien a, b, c von 0 verschiedene ganze Zahlen. Unter einer Lösung von (1) verstehen wir stets eine ganzzahlige Lösung $(x, y, z) \in \mathbb{Z}^3$ mit $(x, y, z) \neq (0, 0, 0)$. Es ist klar, dass genau dann eine ganzzahlige Lösung existiert, wenn es eine rationale Lösung $(x, y, z) \in \mathbb{Q}^3 \setminus \{(0, 0, 0)\}$ gibt. Bei der Behandlung der Legendre-Gleichung kann man sich auf den Fall beschränken, dass die Koeffizienten quadratfrei sind, denn mit $a = a_1\alpha^2,\ b = b_1\beta^2,\ c = c_1\gamma^2$ ist

$$ax^2 + by^2 + cz^2 = a_1(\alpha x)^2 + b_1(\beta y)^2 + c_1(\gamma z)^2$$

Für den Beweis des Drei-Quadrate-Satzes brauchen wir nur folgenden Spezialfall.

12.1. Satz (Legendre). *Seien $a, b \in \mathbb{Z} \setminus \{0\}$ quadratfreie, teilerfremde ganze Zahlen, die nicht beide negativ sind. Genau dann besitzt die Gleichung*

$$ax^2 + by^2 = z^2 \tag{2}$$

eine Lösung $(x, y, z) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$, wenn folgende Bedingungen erfüllt sind:

i) *a ist ein Quadrat modulo b,*

ii) *b ist ein Quadrat modulo a.*

Beweis.

a) Zur Notwendigkeit der Bedingungen. In diesem Teil des Beweises wird nicht benutzt, dass a und b teilerfremd sind.

Sei (x, y, z) eine primitive Lösung, d.h. x, y, z haben keinen gemeinsamen Primeiler. Wir zeigen, dass dann x und b teilerfremd sind. Denn ein gemeinsamer Primteiler p von x und b wäre auch ein Teiler von z. Aus (2) folgt dann $p^2 \mid by^2$, und weil b quadratfrei ist, $p \mid y$, im Widerspruch zur Primitivität der Lösung.

Aus (2) folgt

$$ax^2 \equiv z^2 \bmod b.$$

Da x invertierbar modulo b ist, bedeutet dies, dass a ein Quadrat modulo b ist. Ebenso zeigt man, dass b ein Quadrat modulo a ist.

b) Seien jetzt umgekehrt die Bedingungen (i) und (ii) vorausgesetzt, d.h. es gebe ganze Zahlen u_0, v_0 mit

$$u_0^2 \equiv a \bmod b \quad \text{und} \quad v_0^2 \equiv b \bmod a.$$

Da a und b teilerfremd sind, gibt es nach dem Chinesischen Restsatz ganze Zahlen u, v mit

$$u \equiv u_0 \bmod b,\ u \equiv 0 \bmod a \quad \text{und} \quad v \equiv v_0 \bmod a,\ v \equiv 0 \bmod b,$$

also

$$u^2 \equiv a \bmod ab, \quad uv \equiv 0 \bmod ab, \quad v^2 \equiv b \bmod ab.$$

Mit ganzzahligen Variablen x, y gilt deshalb

$$(ux + vy)^2 \equiv (ax^2 + by^2) \bmod ab.$$

Es folgt

$$(3) \qquad (ux + vy - z)(ux + vy + z) \equiv (ax^2 + by^2 - z^2) \bmod ab.$$

Wir bestimmen jetzt eine "kleine" Lösung der Kongruenz

$$(4) \qquad ux + vy - z \equiv 0 \bmod ab.$$

Dazu betrachten wir die Menge

$$S := \{(x, y, z) \in \mathbb{Z}^3 : 0 \leqslant x < \sqrt{|b|},\ 0 \leqslant y < \sqrt{|a|},\ 0 \leqslant z < \sqrt{|ab|}\}.$$

Wir können annehmen, dass $a \neq 1$ und $b \neq 1$ (da für $a = 1$ oder $b = 1$ die Lösbarkeit von (2) trivial ist). Dann ist $|ab| > 1$ keine Quadratzahl, also $\sqrt{|ab|}$ keine ganze Zahl. Daraus folgt, dass S mehr als $|ab|$ Gitterpunkte enthält. Nach dem Dirichletschen Schubfachprinzip gibt es daher zwei verschiedene Vektoren $(x_i, y_i, z_i) \in S$ mit

$$ux_1 + vy_1 - z_1 \equiv ux_2 + vy_2 - z_2 \bmod ab.$$

Die Differenz $(x,y,z) := (x_1 - x_2, y_1 - y_2, z_1 - z_2) \neq (0,0,0)$ erfüllt dann (4) und es gilt

$$(5) \qquad |a|x^2 < |ab|, \quad |b|y^2 < |ab|, \quad z^2 < |ab|.$$

Aus (3) und (4) folgt jetzt

$$ax^2 + by^2 - z^2 \equiv 0 \bmod ab,$$

und wegen (5) ist

$$|ax^2 + by^2 - z^2| < 2|ab|.$$

Aufgrund der möglichen Vorzeichen von a und b überlegt man sich, dass nur die beiden Fälle

$$(6)_2^1 \qquad ax^2 + by^2 - z^2 = \begin{cases} 0 \\ ab \end{cases}$$

auftreten können. Im ersten Fall sind wir fertig. Im zweiten Fall schließen wir so weiter: Aus $(6)_2$ ergibt sich

$$(7) \qquad ax^2 - ab = a(x^2 - b) = z^2 - by^2.$$

Mit der Normfunktion

$$\mathrm{N}(s + t\sqrt{b}) := (s + t\sqrt{b})(s - t\sqrt{b}) = s^2 - bt^2$$

im Zahlring $\mathbb{Z}[\sqrt{b}]$ lässt sich (7) auch so schreiben:

$$a\mathrm{N}(x + \sqrt{b}) = \mathrm{N}(z + y\sqrt{b}).$$

Multipliziert man dies mit $x_1 := \mathrm{N}(x + \sqrt{b})$, so erhält man wegen der Multiplikativität der Norm

$$ax_1^2 = \mathrm{N}\left((z + y\sqrt{b})(x + \sqrt{b})\right) = \mathrm{N}\Big((zx + by) + (z + xy)\sqrt{b})\Big) = z_1^2 - by_1^2,$$

wobei $z_1 := zx + by$, $y_1 := z + xy$. Wir haben damit eine Lösung der Gleichung (2) gefunden, q.e.d.

Wir kommen jetzt zur Darstellung einer natürlichen Zahl als Summe von drei Quadratzahlen. Dies ist nicht immer möglich. Z.B. ist leicht zu sehen, dass die Zahl 7 sich nicht als Summe von drei Quadratzahlen darstellen lässt. Die genaue Bedingung wird durch den folgenden Satz gegeben.

12.2. Satz (Drei-Quadrate-Satz von Gauß). *Eine positive ganze Zahl n ist genau dann Summe dreier Quadratzahlen,*

$$(*) \qquad n = x_1^2 + x_2^2 + x_3^2, \qquad x_i \in \mathbb{Z},$$

wenn $n = 4^k m$ mit $4 \nmid m$ und $m \not\equiv 7 \bmod 8$.

Wir zeigen jetzt kurz die Notwendigkeit der Bedingungen. Das Quadrat einer ganzen Zahl nimmt modulo 8 nur die Werte 0,1,4 an. Daraus folgt, dass eine natürliche Zahl $n \equiv 7 \bmod 8$ nicht die Summe dreier Quadratzahlen sein kann. Es ist also nur noch zu zeigen: Ist $4n$ eine Summe von drei Quadraten, so auch n. Dies sieht man so: Ist $4n = x_1^2 + x_2^2 + x_3^2$, so müssen alle x_i gerade sein, und n ist Summe der Quadratzahlen $(x_i/2)^2$.

Dass die Bedingungen auch hinreichend sind, können wir erst nach einigen Vorbereitungen beweisen.

Der folgende Satz zeigt, dass es genügt, eine Abschwächung der Gleichung $(*)$ zu lösen.

12.3. Satz (L. Aubry). *Sei n eine natürliche Zahl. Genau dann besitzt die Gleichung*

$$n = x_1^2 + x_2^2 + x_3^2$$

eine ganzzahlige Lösung $(x_1, x_2, x_2) \in \mathbb{Z}^3$, wenn die Gleichung

$$nt^2 = x_1^2 + x_2^2 + x_3^2$$

eine nicht-tiviale Lösung $(t, x_1, x_2, x_2) \in \mathbb{Z}^4$ besitzt.

Beweis. Wir benutzen die Abkürzungen

$$\|x\|^2 := \sum_{i=1}^{3} x_i^2 \quad \text{und} \quad \langle x, y\rangle := \sum_{i=1}^{3} x_i y_i$$

für $(x_1, x_2, x_3), (y_1, y_2, y_3) \in \mathbb{Z}^3$. Sei

$$nt^2 = \|x\|^2, \quad (t, x) \in \mathbb{Z} \times \mathbb{Z}^3, \quad t \neq 0.$$

Wir können $t > 0$ annehmen. Falls $t = 1$, sind wir fertig. Sei also $t > 1$. Es genügt offenbar, ein $t' \in \mathbb{Z}$ und ein $x' \in \mathbb{Z}^3$ zu finden mit $1 \leqslant t' < t$ und $nt'^2 = \|x'\|^2$.

Wir teilen x_ν durch t mit absolut kleinstem Rest:

$$x_\nu = ty_\nu + z_\nu, \quad y_\nu, z_\nu \in \mathbb{Z}, \quad |z_\nu| \leqslant \tfrac{1}{2}\, t.$$

Für die Vektoren $y = (y_1, y_2, y_3), z = (z_1, z_2, z_3) \in \mathbb{Z}^3$ gilt dann

$$x = ty + z, \quad \|z\|^2 \leqslant \tfrac{3}{4}\, t^2.$$

Falls $z = 0$, sind wir fertig, denn dann ist $n = \|y\|^2$. Sei nun $z \neq 0$. Es ist

$$nt^2 = \|x\|^2 = t^2\|y\|^2 + 2t\langle y, z\rangle + \|z\|^2.$$

Daraus folgt, dass $\|z\|^2$ durch t teilbar ist,

$$\|z\|^2 = tt' \quad \text{mit } t' \in \mathbb{Z}, \quad 0 < t' \leqslant \tfrac{3}{4}\, t.$$

Setzen wir dies in die vorige Gleichung ein, so erhalten wir nach Kürzung durch t

$$t\,(n - \|y\|^2) = 2\langle y, z\rangle + t'.$$

Mit der Abkürzung $\gamma := n - \|y\|^2$ haben wir

$$2\langle y, z\rangle = t\gamma - t'.$$

Behauptung. Für den Vektor $x' := t'y - \gamma z$ gilt

$$nt'^2 = \|x'\|^2.$$

Beweis hierfür.

$$\begin{aligned} \|x'\|^2 &= t'^2\|y\|^2 - 2t'\gamma\langle y, z\rangle + \gamma^2\|z\|^2 \\ &= t'^2\|y\|^2 - t'\gamma(t\gamma - t') + \gamma^2 tt' \\ &= t'^2\|y\|^2 + t'^2\gamma = nt'^2, \qquad \text{q.e.d.} \end{aligned}$$

Damit ist Satz 12.3 bewiesen. Aus Satz 12.1 können wir nun das entscheidende Hilfsmittel zum Beweis des Drei-Quadrate-Satzes herleiten.

12.4. Lemma. *Sei n eine quadratfreie natürliche Zahl.*

a) *Falls $n \equiv 1 \bmod 4$ oder $n \equiv 2 \bmod 4$, gibt es eine Primzahl $p \equiv 1 \bmod 4$, so dass die Legendresche Gleichung*

$$nx^2 - py^2 = z^2 \tag{8}$$

lösbar ist.

b) *Falls* $n \equiv 3 \bmod 8$*, gibt es eine Primzahl* $p \equiv 1 \bmod 4$*, so dass die Legendresche Gleichung*

$$nx^2 - 2py^2 = z^2 \tag{9}$$

lösbar ist.

Beweis. Der Beweis benutzt den Dirichletschen Primzahlsatz: Sind k, m teilerfremde natürliche Zahlen, so gibt es unendlich viele Primzahlen p mit

$$p \equiv k \bmod m.$$

a1) Wir behandeln zuerst den Fall, dass $n \equiv 1 \bmod 4$.

Nach dem Dirichletschen Primzahlsatz gibt es eine Primzahl p mit

$$p \equiv 2n - 1 \bmod 4n$$

Damit ist $p \equiv 1 \bmod 4$ und p zu n teilerfremd. Nach Satz 12.1 ist deshalb nur noch zu zeigen:

(i) n ist ein Quadrat modulo p.
(ii) $-p$ ist ein Quadrat modulo n.

Zu (i) Da $p \equiv -1 \bmod n$, ist

$$\Big(\frac{n}{p}\Big) = \Big(\frac{p}{n}\Big) = \Big(\frac{-1}{n}\Big) = (-1)^{(n-1)/2} = 1.$$

Dabei wurde das quadratische Reziprozitätsgesetz benutzt.

Zu (ii) Da $-p \equiv 1 \equiv 1^2 \bmod n$, ist $-p$ ein trivialerweise ein Quadrat modulo n.

a2) Sei jetzt $n \equiv 2 \bmod 4$. Wir wählen eine Primzahl p mit

$$p \equiv n - 1 \bmod 4n$$

Wieder ist $p \equiv 1 \bmod 4$ und p zu n teilerfremd. Außerdem gilt $p \equiv -1 \bmod n$. Wir setzen $n = 2m$. Dann ist m ungerade. Es gilt

$$\Big(\frac{n}{p}\Big) = \Big(\frac{2}{p}\Big)\Big(\frac{m}{p}\Big) = \Big(\frac{2}{p}\Big)\Big(\frac{p}{m}\Big) = \Big(\frac{2}{p}\Big)\Big(\frac{-1}{m}\Big).$$

Wir unterscheiden jetzt zwei Fälle:

Falls $m \equiv 1 \bmod 4$, folgt $n \equiv 2 \bmod 8$, also $p \equiv 1 \bmod 8$. Dann ist $(\frac{-1}{m}) = 1$ und $(\frac{2}{p}) = 1$ (nach dem 2. Ergänzungssatz zum Reziprozitätsgesetz). Daraus folgt $(\frac{n}{p}) = 1$, d.h. die Bedingung (i) ist erfüllt.

Falls $m \equiv 3 \bmod 4$, folgt $n \equiv 6 \bmod 8$, also $p \equiv 5 \bmod 8$. Dann ist $(\frac{-1}{m}) = -1$ und $(\frac{2}{p}) = -1$, also $(\frac{n}{p}) = 1$, d.h. die Bedingung (i) ist ebenfalls erfüllt.

Wegen $-p \equiv 1 \bmod n$ ist $-p$ ein Quadrat modulo n. Nach Satz 12.1 ist deshalb (8) lösbar.

b) Falls $n \equiv 3 \bmod 8$, ist $n-2$ zu $4n$ teilerfremd, es gibt deshalb eine Primzahl p mit

$$p \equiv n - 2 \bmod 4n.$$

Wieder ist $p \equiv 1 \bmod 4$ und p zu n teilerfremd. Es gilt

$$\Big(\frac{n}{p}\Big) = \Big(\frac{p}{n}\Big) = \Big(\frac{-2}{n}\Big) = \Big(\frac{-1}{n}\Big)\Big(\frac{2}{n}\Big) = (-1)(-1) = 1.$$

Daraus folgt: n ist Quadrat modulo p, also auch modulo $2p$.

Da $p \equiv -2 \bmod n$, folgt $-2p \equiv 4 \bmod n$, also ist $-2p$ ein Quadrat modulo n.

Daher ist nach Satz 12.1 die Gleichung (9) lösbar.

Beweis des Drei-Quadrate-Satzes

Es genügt, den Satz für quadratfreies n zu beweisen. Denn aus $n = mk^2$ mit einer ungeraden Zahl k folgt $n \equiv m \bmod 8$.

Sei also n eine natürliche Zahl mit $n \not\equiv 0, 4, 7 \bmod 8$.

Falls $n \equiv 1, 2, 5, 6 \bmod 8$, können wir nach Lemma 12.4 eine Primzahl $p \equiv 1 \bmod 4$ finden, so dass die Gleichung

$$nx^2 - py^2 = z^2$$

eine nicht-triviale ganzzahlige Lösung besitzt. Da $p \equiv 1 \bmod 4$, ist p Summe zweier Quadratzahlen, $p = u^2 + v^2$, $u, v \in \mathbb{Z}$. Es folgt

$$nx^2 = z^2 + (uy)^2 + (vy)^2.$$

Aus Satz 12.3 folgt nun, dass n Summe dreier Quadratzahlen ist.

Im verbleibenden Fall $n \equiv 3 \bmod 8$ gibt es nach Lemma 12.4 eine Primzahl $p \equiv 1 \bmod 4$, so dass die Gleichung

$$nx^2 - 2py^2 = z^2$$

eine nicht-triviale ganzzahlige Lösung besitzt. Auch $2p$ ist Summe zweier Quadratzahlen, denn aus $p = u^2 + v^2$ folgt $2p = (u+v)^2 + (u-v)^2$. Also kann man weiter wie oben schließen.

Damit ist der Drei-Quadrate-Satz bewiesen.

Übrigens ist der Vier-Quadrate-Satz von Lagrange eine einfache Folgerung aus dem Drei-Quadrate-Satz. Denn entweder ist eine natürliche Zahl n schon Summe von drei Quadraten oder von der Form $n = 4^k m$ mit $m \equiv 7 \bmod 8$. Dann ist aber $n - (2^k)^2 = 4^k(m-1)$ Summe von drei Quadraten und deshalb n Summe von vier Quadraten.

Dreieckszahlen. Unter einer Dreieckszahl versteht man eine natürliche Zahl der Gestalt

$$\Delta_m := \sum_{k=1}^{m} k = \frac{m(m+1)}{2}.$$

12.5. Corollar. *Jede natürliche Zahl n ist Summe von drei Dreieckszahlen.*

Beweis. Die Zahl $N := 8n + 3$ ist nach Satz 12.2 Summe von drei Quadratzahlen, die notwendig alle ungerade sind:

$$\begin{aligned} N = 8n + 3 &= \sum_{i=1}^{3} (2m_i + 1)^2 = \sum_{i=1}^{3} (4m_i^2 + 4m_i + 1) \\ &= 8 \sum_{i=1}^{3} \frac{m_i(m_i+1)}{2} + 3, \end{aligned}$$

also

$$n = \Delta_{m_1} + \Delta_{m_2} + \Delta_{m_3}, \qquad \text{q.e.d.}$$